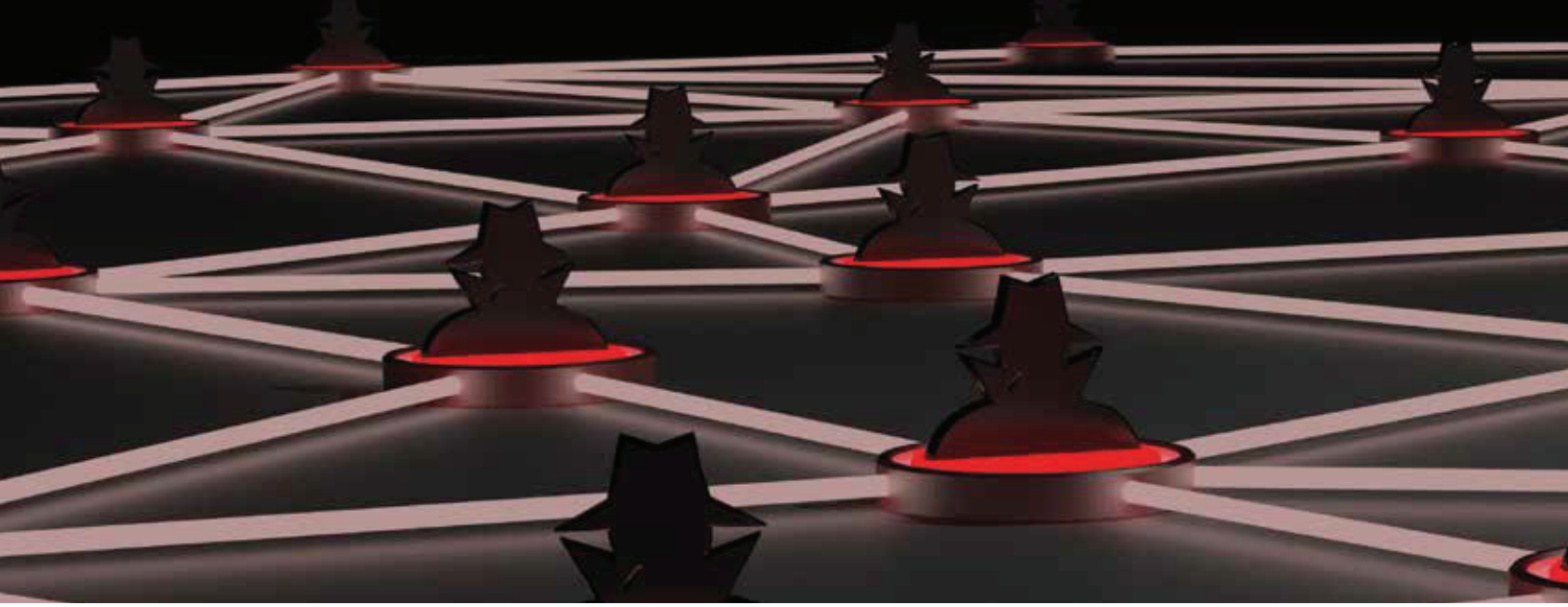
CYBERATTACK

PREPAREDNESS DECODED: PREVENTION AND MITIGATION

by Mitchell Ayes and Jesse Lubin

In recent years, some of the largest organizations in the United States—including Google, Facebook, Marriott International, Equifax, and Anthem (the nation's second largest health insurer)—have reported vast data breaches. Although these organizations have already experienced significant financial ramifications, it will take several years to determine the full amount of damages. This article explores two of these breaches and various methods of prevention. It also discusses some insurance options available to protect against a cyberattack.



In November 2018, Marriott International reported that, over the course of four years, hackers stole approximately 500 million records from its Starwood Hotels reservation system.[1] Marriott confirmed that the breach exposed the personal data of its customers, including their passport and credit card numbers. Shares of Marriott immediately fell, but the long-term damage may not be known for several years.

A recent study sponsored by IBM Security and conducted by the Ponemon Institute revealed that the hidden costs of data breaches can include, among other things, lost business, a negative impact on the organization's reputation, and time spent by employees to remediate the breach.[2] Unsurprisingly, the study indicates that one-third of the cost of a megabreach (a breach in which more than 1 million records are stolen) is derived from lost business. The study estimated that megabreaches cost organizations an average of nearly $40 million for every 1 million compromised records. The study also noted that the average time an organization takes to identify a data breach is 197 days. It is worth noting that Marriott took four years to discover its breach.

Megabreaches cost organizations an average of nearly $40 million for every 1 million compromised records

After Marriott's breach, the company reported that it carried cybersecurity liability insurance, but it did not disclose the amount of coverage. Marriott admitted that its coverage "may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches." Marriott further stated that "in the future, such insurance may not be available to [them] on commercially reasonable terms, or at all." [3]

When credit-monitoring company Equifax initially reported that a data breach affected 145.5 million U.S. consumers, it disclosed that it maintained $125 million of cybersecurity insurance coverage with a $7.5 million deductible. While that coverage may sound reasonable, Equifax spent $430.5 million on breach-related expenses through November 2018.[4]

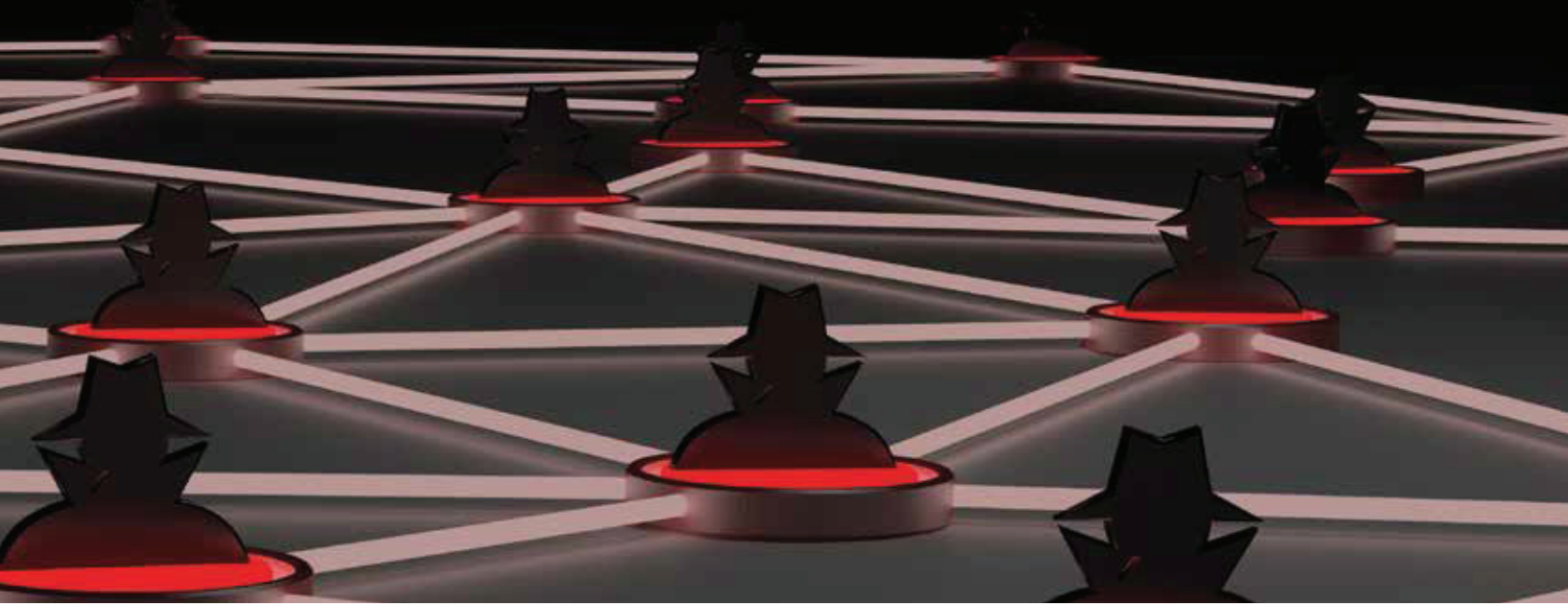
PLANNING FOR A DATA BREACH

To protect themselves, their employees, their customers, and the sensitive data they maintain, organizations must enact prebreach and postbreach plans.

Think back to when you experienced your first fire drill as a kindergarten student. Your teacher likely explained to you and the other students how to conduct yourselves during the fire drill and how to return safely to the classroom after the drill. Organizations should also think this way to prevent and counteract a cyberattack. While organizations need to lead the way by developing and implementing an effective prevention plan, their employees, just like the kindergarten students, need to execute the plan to ensure data is safe and secure.

To effectively mitigate the risks of a cyberattack, an organization must first determine what data and information could be subject to a data breach.[5] It should identify what first-party data (its own proprietary data) and third-party data (its customers' data) should be safeguarded.[6] Knowing this information can help the organization implement an effective strategy. Organizations that collect customers' sensitive information—whether personal, health, financial, or business information—have a responsibility to protect it.

Next, organizations must install reliable spam filters and virus and malware protection software and block known malicious websites from employee use. Organizations should encrypt their sensitive files, enable multifactor authentication (for example, sending a text message with a numerical code for the user to enter in his or her browser to gain access to a certain website or account), and continuously monitor their own enterprise information technology (IT)



footprint and endpoints (internet-capable devices such as computers and cell phones). Sensitive information should be backed up regularly. This includes checking the integrity of the data to ensure that files are accurate and complete and can be restored efficiently.[7]

Organizations must also ensure that their vendors are aware of their breach-preparedness protocols and must require strong contractual indemnification language in case a vendor breach occurs. It is also important for organizations to periodically complete a stress test to find their most vulnerable areas for attack and to implement procedures to secure these areas.

Further, organizations must have a competent breach-response team in place to preserve and protect any unexposed data and to obtain evidence to determine how the breach occurred and who is responsible. The breach-response team should be composed of outside legal counsel, forensic experts, the organization's insurance company, and possibly a public relations firm, depending on the scale of the breach, so that an emergency response plan can be initiated at the first notice of a breach.

RESPONDING TO A DATA BREACH

Once a breach occurs, an organization must promptly respond to it. Some jurisdictions have notice provisions that mandate an organization to notify its customers about the breach and to specify what data may have been compromised.

The organization must determine where the breakdown in its security protocols occurred, whether there was any authorized access by its employees, where other vulnerabilities exist, and what upgrades are necessary. This is the reason schools have fire drills and organizations have stress tests—to determine how to protect themselves in the event of a disaster.

PROTECTING AGAINST A DATA BREACH

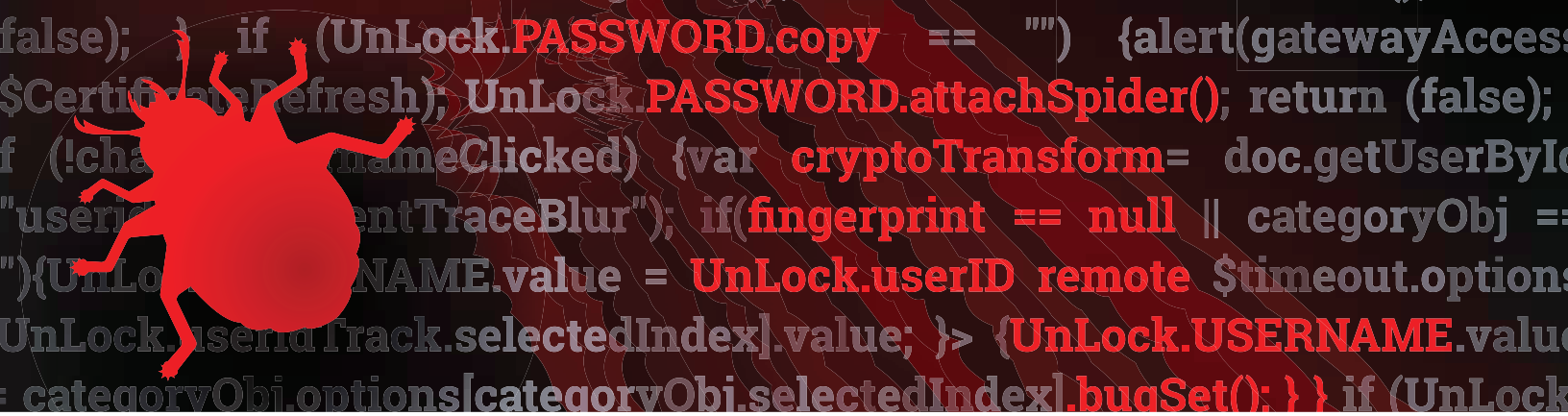
While organizations are responsible for protecting themselves against potential malicious attacks, their employees are the first line of defense. Organizations can minimize liability associated with cyber breaches by educating their employees about how breaches can occur. For example, hackers often target employees by sending emails or pop-ups containing links to malware. Phishing attacks send emails, purportedly from a reputable source, requesting sensitive or personal information, such as Social Security, credit card, or bank account numbers.

While organizations are responsible for protecting themselves against potential malicious attacks, their employees are the first line of defense

Employees must be trained to not only recognize the potential for these cyberattacks but also how to prevent them and minimize exposure. Organizations can train employees to apply these relatively easy safety measures to vastly improve cybersecurity: create secure passwords, back up sensitive data, perform regular software updates, use caution, and lock computers when away from them.[8]

Poor password practices can make entire organizations vulnerable to a breach. All employees should create strong, unique, and unpredictable passwords. They should never use the same password for more than one program or website because hackers who determine that password can use it to access all of them. While employees may grumble about how many passwords they have to remember, they don't want to be the reason an organization accidentally releases 500 million records.

Corporate policy should mandate that employees back up sensitive data on a separate drive. If employees save a significant amount of data or sensitive information on a computer that is subsequently hacked, the hacker could install ransomware, which holds that data hostage until a ransom is paid. In other words, ransomware could deprive an organization of its data unless it pays the hacker for its return. To avoid this, employees should be required to save copies of their data in separate secure locations, such as on a different hard drive or in a cloud.



Organizations must also instruct employees to perform software updates when they are prompted by the operating system to do so and antivirus software updates, which may include updated protection from spyware, botnets, phishing emails, and other viruses. Software updates usually do not take long to install, and it's critical to keep up with them. Operating systems are often updated by their manufacturer as soon as they detect a vulnerability, and antivirus software can be updated for each new virus that's discovered.

The most important safety measure for employees is to remain vigilant and use common sense. Employees' best defense against cyberattacks is caution. For example, they should always determine who an email is from before opening it. They should never open an email attachment without knowing who it's from and what it is. If employees have any questions regarding an attachment, they should contact the sender before they open it to confirm that the attachment is a safe document.

Lastly, employees should lock or shut down their computer any time they are away from it so that nobody else can access it.

Employees' best defense against cyberattacks is caution

Many of the safety measures that can help minimize the risk of a cyber breach are common sense. However, it's a good idea to remind employees to perform these measures on a regular basis.

An organization reduces its exposure and potential liability by implementing safety measures that protect itself, its employees, and its customers from experiencing a cyber breach. Just like the fire drill from kindergarten, organizations and their employees must continue to work together to develop, implement, modify, and maintain plans that protect organizations from cyberattacks.

INSURANCE SOLUTIONS

Insurance solutions are available for organizations that could be exposed to first- or third-party cyberattacks. Data breach policies cover various penalties, legal costs, and fines (for example, for Health Insurance Portability and Accountability Act [HIPAA] violations) arising from data breaches. The policies are also designed to cover postbreach costs such as credit monitoring (for financial data breaches) and expenses related to notifying customers of a breach.

Insurance products can also cover privacy and security liabilities that may arise when victims claim that an organization didn't do enough to prevent a breach. Some policies even cover the costs associated with recovering and replacing data that has been lost, damaged, or corrupted.

There are various ways organizations can protect themselves from data breaches and minimize liability to others for a failure to do so. However, just like in the cases of Equifax and Marriott International, when a breach does occur, the associated postbreach costs can be immense. Organizations should consider the amount of data they are required to protect and secure cyberbreach insurance policies with coverage limits high enough to adequately insulate themselves from financial harm. ■

Many thanks to the Risk Management Interest Group for its contributions to this article.

1. Jim Finkle, "Marriot Starwood Assessing Impact of 4-Year Long Data Breach," *Insurance Journal,* November 30, 2018, www.insurancejournal.com/news/national/2018/11/30/510662.htm (accessed May 1, 2019).
2. IBM and Ponemon Institute, "2018 Cost of a Data Breach Study: Global Overview," July 2018, www.ibm.com/downloads/cas/861MNWN2 (accessed May 1, 2019).
3. Bala Yogesh, "Cybersecurity Trends 2018: Year of Regulations and Breaches," *Security Investing News*, December 12, 2018, https://investingnews.com/daily/tech-investing/cybersecurity-investing/cybersecurity-trends/ (accessed May 1, 2019).
4. Larry Dignan, "Marriott faces massive data breach expenses even with cybersecurity insurance," November 30, 2018, www.zdnet.com/article/marriott-faces-massive-data-breach-expenses-even-with-cybersecurity-insurance/ (accessed May 1, 2019).
5. MetricStream, "Five Steps to Mitigate the Risks of Increasing Cyber Attacks in Healthcare," www.metricstream.com/insights/mitigate-risks-of-increasing-cyber-attacks.htm (accessed May 1, 2019).
6. Sungard Availability Services, "5 Steps to Assess and Mitigate Cyber Security Risks," www.sungardas.com/en/about/resources/articles/5-steps-to-assess-and-mitigate-cyber-security-risks/ (accessed May 1, 2019).
7. Alniz Popat, "Five Ways to Protect Your Company Against Cyber Attacks," *Entrepreneur*, July 19, 2018, www.entrepreneur.com/article/316886 (accessed May 1, 2019).
8. Popat, "Five Ways to Protect Your Company Against Cyber Attacks."